

**REMARKS**

Applicants respectfully request reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

**Status of Claims:**

No claims are currently being cancelled.

Claims 1 and 7 are currently being amended.

Claims 13 and 14 are currently being added.

This amendment and reply adds and amends claims in this application. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claims remain under examination in the application, is presented, with an appropriate defined status identifier.

After adding and amending the claims as set forth above, claims 1-14 are now pending in this application.

**Claim Rejections – Prior Art:**

In the Office Action, claims 1-12 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Publication No. 2002/0191572 to Weinstein et al. This rejection is traversed with respect to the presently pending claims under rejection, for at least the reasons given below.

Presently pending independent claim 1 now recites, among other things:

*when a user subscribed to the communication service system accesses the predetermined access point, payload processing is executed using a processing method unique to each user, and each user is discriminated based on data of the processed parts such that none of the users is capable of intercepting payload data of any of other users currently accessing the predetermined access point, due to differences in payload processing techniques respectively utilized by the payload processing methods respectively provided for each user.*

While Weinstein describes a public access mobility LAN and method, it appears that the payload processing method assigned to each of the users of a hot spot in the system of Weinstein is the same processing method, and thus one user can in theory hack into another

user's payload (either uplink or downlink). It is noted that paragraph 0098 of Weinstein describes the use of IPSEC encapsulated security payload to encrypt an IP payload, and whereby this encryption allows each user to securely use a hot spot without worrying about other users trying to hack into the user's data. However, the IPSEC encapsulated security payload system is a single method, and does not correspond to the claimed different methods assigned to different users in the presently claimed invention. The fact that one user may be assigned a different private key/public key pair from another user in the system of Weinstein does not change the fact that those two users are using the same payload processing method.

Accordingly, presently pending independent claim 1, as well as presently pending independent claim 7 that has been amended in a similar manner, are not anticipated by Weinstein.

Still further, with respect to the rejection of dependent claims 3 and 9, the Office Action asserts that paragraphs 0043 and 0098 of Weinstein discloses the features recited in those claims. Applicant respectfully disagrees. Namely, claims 3 and 9 recite that one of a plurality of preliminarily prepared processing methods is randomly selected for the payload processing. Paragraph 0043 of Weinstein merely describes that a plurality of LAN segments are utilized, whereby virtual operators could be any third-party provider, such as a cellular mobile operator. This has nothing at all to do with randomly selecting preliminarily prepared processing methods for payload processing. Paragraph 0098 of Weinstein describes the use of IPSEC encapsulated security payload to encrypt an IP payload for each user assigned to a hot spot, whereby this also has nothing at all to do with randomly selecting preliminarily prepared processing methods for payload processing (note that each user is assigned the same processing method, that being IPSEC, the fact that each user may have a different private/public key does not alter this fact).

Accordingly, dependent claims 3 and 9 are not anticipated by Weinstein for these additional reasons, beyond the reasons given above for their respective base claim.

**New Claims:**

New claims 13 and 14 have been added, whereby these claims are believed to patentably distinguish over the cited art of record.

In particular, new independent claim 13 recites:

*A wireless network service provision method of providing communication services including internet connection by permitting access to a predetermined access point in a limitative area via wireless LAN or local wireless interface, the method comprising:*

*accessing, by a new user subscribed to the communication service system, the predetermined access point;*

*assigning one of a plurality of data processing methods to the new user, the one of the plurality of data processing methods being different from other ones of the data processing methods that have been respectively assigned to other users currently accessing the predetermined access point,*

*wherein none of the users currently accessing the predetermined access point is capable of intercepting data being uploaded by or downloaded to the new user, due to differences in payload processing with respect to the plurality of data processing methods assigned to each of the users.*

Weinstein does not disclose or suggest the features in the assigning step and the wherein clause of new claim 13, whereby, at best, Weinstein merely describes that each user is secure from data tampering from other users by way of the same encryption scheme (albeit with different public and private keys) that each user utilizes while using the hot spot. Thus, there is no assigning of a data processing method that is different from other data processing methods that have been previously assigned to other users in the system of Weinstein.

New dependent claim 14 recites additional features of the assigning step that are not disclosed or suggested by Weinstein. For example, Weinstein does not disclose or suggest determining which ones of the plurality of data processing methods are currently not assigned to any users and are thus available for assignment to new users, as available data processing methods. Rather, Weinstein merely assigns the same encryption method to each new user coming into the system, as described in paragraph 0098 of Weinstein.

**Conclusion:**

Since all of the issues raised in the Office Action have been addressed in this Amendment and Reply, Applicants believe that the present application is now in condition for allowance, and an early indication of allowance is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check or credit card payment form being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicants hereby petition for such extension under 37 C.F.R. §1.136 and authorize payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date November 27, 2007

FOLEY & LARDNER LLP  
Customer Number: 22428  
Telephone: (202) 945-6014  
Facsimile: (202) 672-5399

By Phillip J. Articola

George C. Beck  
Registration No. 38,072

Phillip J. Articola  
Registration No. 38,819